OSINT + ARCO + PROTECCIÓN DE DATOS

MAPA-RD: Exposición y Ruta de Cierre

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecutable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

Felipe de Jesús Miramontes Romero · Reporte RPT-2026-020 · 2026-01-20

Reporte Ejecutivo de Seguridad · Exposición pública · Estrictamente Confidencial

Índice de Riesgo Digital

Evaluación Cuantitativa de Postura (Estado Global)

Diagnóstico Operativo

Urgencia Inmediata: Un IRD de 94 señala un **Máximo riesgo sistémico**. Datos sensibles (financieros/accesos) están expuestos activamente. Se requiere **contención de emergencia** para evitar fraude inminente.

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-001

Adobe

89 CRÍTICO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2013-10-04

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Password hints, Passwords, Usernames

Descripción

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-002

000webhost

89 CRÍTICO

Activo:	Tipo:	Fecha:
Identidad Digital	Brecha de Datos	2015-03-01

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, IP addresses, Names, Passwords

Descripción

In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded bef...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-003

Dropbox

87 CRÍTICO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2012-07-01

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Passwords

Descripción

In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password reset...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-004

GeekedIn

70 ALTO

Activo: Identidad Digital

Tipo: Brecha de Datos

Fecha: 2016-08-15

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Geographic locations, Names, Professional skills, Usernames

Descripción

In August 2016, the technology recruitment site GeekedIn left a MongoDB database exposed and over 8M records were extracted by an unknown third party. The breached data was originally scraped from GitHub in violation of their terms of use and contained information exposed in public profiles, includi...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-005

ExploitIn

87 CRÍTICO

Activo:	Tipo:	Fecha:
Identidad Digital	Brecha de Datos	2016-10-13

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Passwords

Descripción

In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "creden...

VEC-006

Collection1

87 CRÍTICO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2019-01-07

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Passwords

Descripción

In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique ...

VEC-007

MyFitnessPal

89 CRÍTICO

Activo:	Tipo:	Fecha:
Identidad Digital	Brecha de Datos	2018-02-01

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, IP addresses, Passwords, Usernames

Descripción

In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords sto...

Vectores De Vulnerabilidad

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-008

Animoto

90 CRÍTICO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2018-07-10

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Dates of birth, Email addresses, Geographic locations, Names, Passwords

Descripción

In July 2018, the cloud-based video making service Animoto suffered a data breach. The breach exposed 22 million unique email addresses alongside names, dates of...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-009

Canva

90 CRÍTICO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2019-05-24

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Geographic locations, Names, Passwords, Usernames

Descripción

In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names,...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-010

123RF

92 CRÍTICO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2020-03-22

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, IP addresses, Names, Passwords, Phone numbers

Descripción

In March 2020, the stock photo site 123RF suffered a data breach which impacted over 8 million subscribers and was subsequently sold online...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-011

Nitro

88 CRÍTICO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2020-09-28

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Names, Passwords

Descripción

In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exp...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-012

Banorte

70 ALTO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2014-08-18

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Account balances, Email addresses, Genders, Government issued IDs, Names

Descripción

In August 2022, millions of records from Mexican bank "Banorte" were publicly dumped on a popular hacking forum including 2.1M unique email addresses, physical addresses, ...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-013

Twitter200M

70 ALTO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2021-01-01

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Names, Social media profiles, Usernames

Descripción

In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing ...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-014

ManipulatedCaiman

70 ALTO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2023-07-16

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses

Descripción

In July 2023, Perception Point reported on a phishing operation dubbed "Manipulated Caiman". Targeting primarily the citizens of Me...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-015

Trello

70 ALTO

Activo:
Identidad Digital

Tipo:
Brecha de Datos

Fecha:
2024-01-16

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

- Email addresses, Names, Usernames

Descripción

In January 2024, data was scraped from Trello and posted for sale on a popular hacking forum. Containing over 15M email addresses, names and usernames, the data was obtained by enumerating a publicl...

Vectores De Vulnerabilidad

Evidencia Técnica y Ruta de Cierre Priorizada

VEC-016

SynthientCredentialStuffingThreatData

87 CRÍTICO

Activo: Identidad Digital

Tipo: Brecha de Datos

Fecha: 2025-04-11

Acciones Recomendadas

- Cambiar contraseñas asociadas inmediatamente.
- Activar 2FA donde sea posible.
- Verificar actividad sospechosa recientes.

Datos Comprometidos

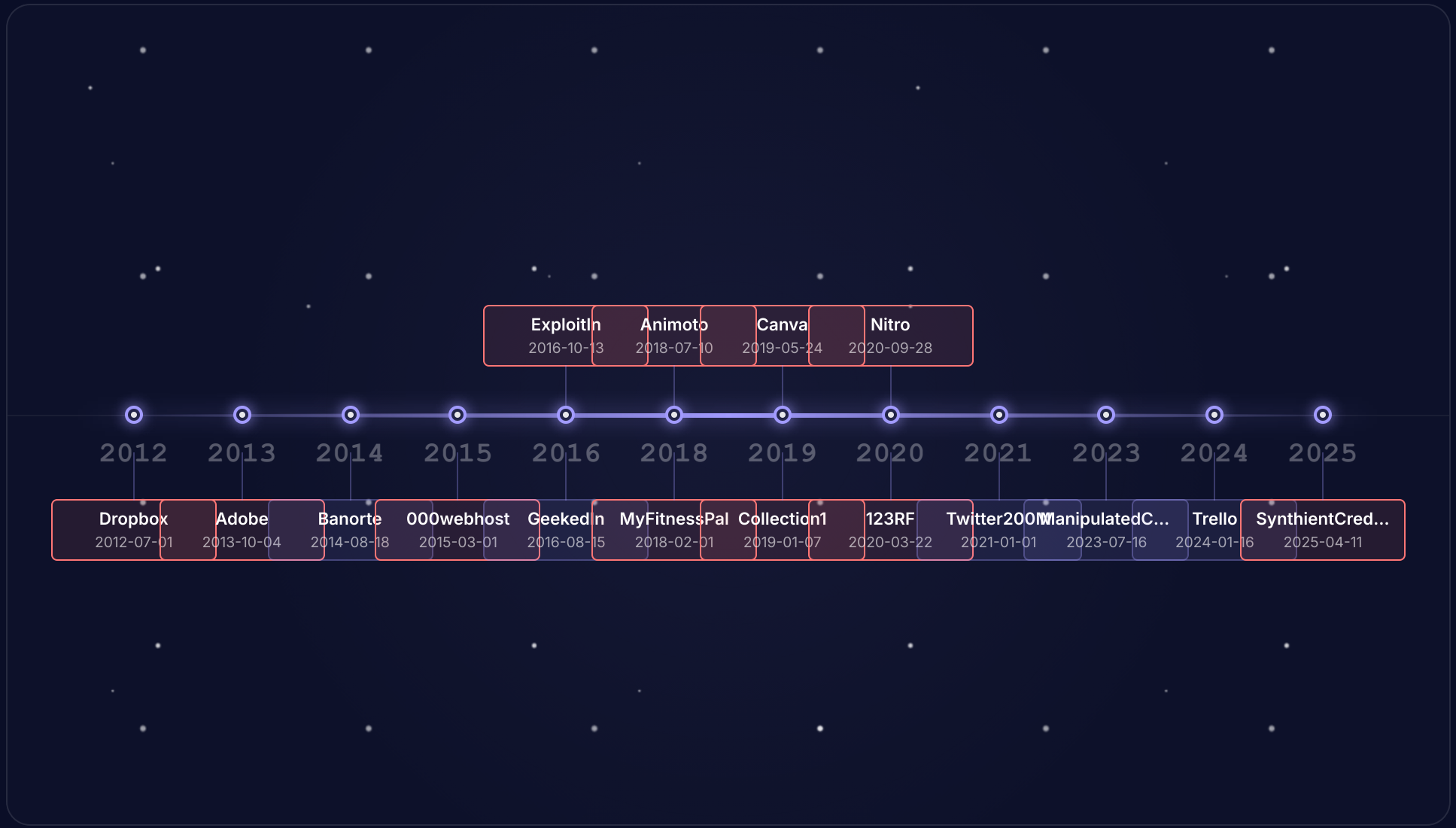
- Email addresses, Passwords

Descripción

During 2025, the threat-intelligence firm Synthient aggregated 2 billion unique email addresses disclosed in credential-stuffing lists found across mu...

Horizonte De Exposición

Cronología de Incidentes Identificados



Valor De Exposición

Estimación de Impacto Financiero en Mercado Negro

CONCEPTO	CANTIDAD	PRECIO UNIT.	SUBTOTAL
Credenciales	12	$15	**$180.00**
Datos Personales	49	$5	**$245.00**
TOTAL ESTIMADO			**$425.00 USD**

Valor Total en Mercado Negro

$425.00 USD

> **Asimetría de Riesgo:** Por una inversión trivial, el mercado negro ofrece las llaves de su organización. Este monto no refleja el valor de sus activos, sino la alarmante facilidad y bajo costo con el que un atacante puede iniciar un incidente catastrófico.

Vector De Ataque

Cómo un atacante usaría esta información

Target

Fase 01

Localización

El atacante utiliza bases de datos públicas para correlacionar tu **Nombre Completo** y **Domicilio** físico, creando un perfil base.

FUENTE EVIDENCIAL

No Public PDF Found

Key

Fase 02

Armado

Validación automatizada de tus credenciales contra servicios financieros. Se configuran scripts con tus **Contraseñas Reales**.

LOG DE MALWARE

No LinkedIn Profile Public

Strike

Fase 03

Impacto

Ejecución del fraude. Acceso no autorizado a banca móvil, suplantación ante el SAT y extracción de recursos financieros.

ESTADO DE RIESGO

Ejecución inminente

Impacto Directo Al Negocio

Traducción de Riesgo Técnico a Estratégico

Financiero

Pérdida directa por fraude bancario, costos elevados de remediación y posibles multas por incumplimiento.

Operativo

Interrupción de servicios críticos, parálisis de sistemas y pérdida de productividad empresarial.

Reputacional

Pérdida catastrófica de confianza del cliente y daño irreversible a la imagen de marca.

Regulatorio

Sanciones legales severas por violaciones a la LFPDPPP, GDPR y normativas de protección.

Escenario De Inacción

La trampa de latencia: por qué no ha pasado nada no significa seguridad

Deuda histórica

13 años sin incidentes

Esto no es seguridad, es suerte operativa. La seguridad por oscuridad funcionaba cuando los ataques eran manuales y dirigidos.

Estado: **Obsoleto**

Nueva visibilidad

Automatización e IA

Hoy, escáneres masivos y bots de IA encuentran vulnerabilidades en segundos. Lo que antes era invisible, ahora es un blanco automático.

Estado: **Expuesto**

Colapso inevitable

Costo exponencial

Sistemas legados sin soporte no se pueden parchar. Una brecha hoy obliga a una reconstrucción total (10x costo) en lugar de remediación.

Estado: **Crítico**

Ventana De Cierre

Plan de acción recomendado para la mitigación de riesgos

Fase 1

0-24 h

Contención inmediata

- **Cambio inteligente de credenciales**

  Implementa una frase de seguridad robusta (ej. MiPerroComeCereal2024) en tu cuenta de correo principal para detener el acceso inmediato.

- **Doble candado (2FA)**

  Activa la verificación en 2 pasos en WhatsApp y banca móvil. Prioriza el uso de una app autenticadora sobre los mensajes SMS.

Fase 2

24-72 h

Ventana táctica

- **Cierre global de sesiones**

  Accede a la configuración de seguridad de Google, Facebook y bancos para forzar el cierre de sesión en todos los dispositivos no reconocidos.

- **Alertas transaccionales totales**

  Configura tu banca móvil para recibir notificaciones por cargos de cualquier monto para detectar intentos de validación de tarjeta.

Fase 3

30 días

Estrategia a largo plazo

- **Candado crediticio (Buró)**

  Solicita el servicio de bloqueo en Buró de Crédito para impedir consultas no autorizadas o apertura de créditos sin tu consentimiento.

- **Higiene digital recurrente**

  Establece una rutina de revisión semanal de estados de cuenta para detectar cargos hormiga antes de un fraude mayor.

Ruta De Cierre Consolidada

Resumen ejecutivo de acciones prioritarias por dominio

Identidad digital

- Cambio de contraseñas del correo principal.
- Activar verificación en 2 pasos (WhatsApp/Email).
- Usar un gestor de claves seguro.
- Revisar qué apps tienen acceso a tu cuenta.
- Borrar cuentas de sitios que ya no usas.

Seguridad financiera

- Bloqueo de consultas en Buró de Crédito.
- Activar notificaciones por cualquier gasto ($0).
- Solicitar reposición de tarjetas expuestas.
- Bajar límites de gasto diario en la App.
- Vincular huella/rostro en la app del banco.

Higiene & privacidad

- Cerrar sesión en todos los dispositivos.
- Ocultar ubicación y datos en redes sociales.
- Revisar estados de cuenta cada semana.
- Imprimir y guardar códigos de recuperación.
- Asegurar teléfono con PIN de 6 dígitos.

Meta de resiliencia — **Nivel proyectado: 95/100**

Nivel de protección estimado tras completar la ruta sugerida en este reporte.

Anexo Técnico

Metodología, Definiciones y Estándares de Cálculo

Índice de Riesgo del Vector (IRV)

El **IRV** es la métrica fundamental de urgencia. No mide el riesgo teórico, sino la necesidad operativa de cierre. Se calcula internamente mediante un modelo ponderado de seis dimensiones.

Fórmula de cálculo

```
IRV = [ Σ(Componente × Peso) / Σ(Peso Máximo) ] × 100
```

Criticidad (CA) x4

Importancia crítica del activo para la continuidad del negocio.

Exposición (ET) x3

Ventana de tiempo y vigencia actual del hallazgo.

Superficie (SE) x3

Facilidad de acceso desde redes públicas o privadas.

Impacto (IM) x4

Suma de impactos (Financiero, Legal, Operativo, Reputacional).

Explotación (FE) x3

Recursos y complejidad técnica requerida para el ataque.

Detección (DV) x3

Probabilidad de evasión de sistemas de monitoreo.

Índice de Riesgo Digital (IRD)

El **IRD** es el indicador de postura global. Se deriva dinámicamente de los vectores activos mediante un promedio ponderado por severidad.

Agregación ponderada

```
IRD = Σ(IRV × Peso Severidad) / Σ(Pesos Severidad)
```

Matriz de pesos (severidad)

Bajo	Medio	Alto	Crítico	Máximo
x1	x2	x3	x4	x5

Anexo Técnico

Referencias, Glosario y Aviso Legal

Stealer Logs

Registros extraídos por malware ("infostealers") que infecta dispositivos personales o corporativos. Estos logs contienen contraseñas guardadas en navegadores, cookies de sesión y datos de autocompletado.

Combo List

Compilaciones masivas de credenciales (usuario:contraseña) provenientes de múltiples brechas de seguridad antiguas y nuevas. Se utilizan para ataques automatizados de "Credential Stuffing" contra diversos servicios.

PII (Personal Identifiable Information)

Cualquier dato que pueda identificar a un individuo específico, como RFC, CURP, dirección física, número de teléfono o huella biométrica. Su exposición facilita el robo de identidad.

Botnet

Red de dispositivos infectados controlados remotamente por un atacante. Los dispositivos "zombis" se usan para robar datos, enviar spam o realizar ataques DDoS sin que el propietario lo sepa.

Texto Plano (Plain Text)

Almacenamiento de contraseñas u otros datos sensibles sin ningún tipo de cifrado o protección matemática. Si la base de datos es vulnerada, los datos son legibles inmediatamente.

Aviso Legal y Limitación de Responsabilidad

Este reporte ha sido generado utilizando técnicas de Inteligencia de Fuentes Abiertas (OSINT) y análisis pasivo de datos públicamente accesibles en "Clear Web", "Deep Web" y "Dark Web".

Naturaleza No Intrusiva: En ningún momento se han realizado ataques activos, intentos de intrusión, ingeniería social o evasión de controles de seguridad contra la infraestructura del Cliente.

Propósito: La información contenida tiene fines estrictamente preventivos y de concienciación. El proveedor no se hace responsable del uso indebido de esta información por terceros.

Confidencialidad: Este documento contiene datos sensibles y está clasificado como ESTRICTAMENTE CONFIDENCIAL.